L Number	Hits	Search Text	DB	Time stamp
-	24	ipsec with classif$7	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 11:50
-	43	ipsec and decrypt$5 near6 parameter	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 11:50
-	10	ipsec and decrypt$5 near6 parameter and classif$8	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 11:53
-	3	ipsec and decrypt$5 near6 parameter and classif$8 near parameter	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 11:58
-	1	6253321.pn. and decrypt$6	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 12:01
-	1	decrypt$6 near6 classif$6 near4 (parameter attribute)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 12:03
-	0	decrypt$6 near6 filter near4 (parameter attribute)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 12:04
-	589	decrypt$6 near6 (parameter attribute)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 12:04
-	45	(decrypt$6 near6 (parameter attribute)) and ipsec	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 13:05
-	12	((decrypt$6 near6 (parameter attribute)) and ipsec) and classif$8	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/07 13:05
-	7	("4715030" | "5172111" | "5448698" | "5561770" | "5615340" | "5761424" | "6092110").PN.	USPAT	2004/09/07 13:27
-	12	decrypt$6 near5 classif$8 with packet	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/08 13:20
-	3375205	GB "2317792"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/08 13:21
-	1	"GB 2317792"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/08 13:21

```
Set     Items   Description
S1      532456   ENCRYPT? OR SCRAMBL? OR CIPHER? OR CRYPT? OR CODE? ? OR EN-
             CIPHER? OR CODING OR CODED OR ENCOD?
S2      170119   DECRYPT? OR DESCRAMBL? OR DECIPHER? OR DECOD? OR UNSCRAMBL?
              OR UNENCOD? OR UNENCRYPT? OR UNCOD? OR UNCIPHER?
S3       27701    (PACKET ? OR FRAME? OR DATAGRAM? OR BLOCK()DATA)(2N)(DATA -
             OR INFORMATION)
S4       89389   S1 (2N) (DATA OR INFORMATION)
S5      975434   CLASSIF? OR CATEGORIZ? OR CATEGORIS? OR CATALOG? OR GROUP?
S6       89389   S1 (2N) (DATA OR INFORMATION)
S7      975434   CLASSIF? OR CATEGORIZ? OR CATEGORIS? OR CATALOG? OR GROUP?
S8      305302   PARAMETER? OR DESCRIPT?()ITEM? OR ATTRIBUT? OR (NAME OR ST-
             RUCTURE? OR SIZE OR VALUE)(2N)(DATA OR INFORMATION)
S9         134   IPSEC OR INTERNET()PROTOCOL()SECURITY
S10      52308    (SECONDARY OR FURTHER OR ADDITIONAL OR NEW OR SUPPLEMENT? -
             OR MORE OR EXTRA?)(2W)(PLACE? OR POSITION? OR LOCATION? OR AR-
             EA? OR SPACE?)
S11     138756    (FIRST OR 1ST OR INITIAL OR LEADING OR CARDINAL OR ORIGINAL
              OR PRIMARY)(2W)(PLACE? OR POSITION? OR LOCATION? OR AREA? OR
             SPACE?)
S12       1460    S1 (2N) S3
S13          0    S9 AND (S2 (2N) S3)
S14         18    S9 AND S2
S15          0    S14 AND S3
S16          0    S12 AND S9
S17        120    S12 AND S7
S18          0    S18 AND S8
S19          0    S18 AND S6
S20          0    S18 AND S2
S21          0    S18 AND S5
S22        134    S9 AND S9
S23          7    S22 AND S7
S24         22    S14 OR S23
S25         22    S24 AND IC=(G06F? OR H04L?)
S26         18    S24 AND MC=(T01-N02A1 OR T01-N02A3B OR T01-N02B2 OR T01-S03
              OR W01-A03B OR W01-A05A OR W01-A06E1 OR W01-A06F OR W01-A06F-
             2A OR W01-A06G2)
S27         22    S25 OR S26
File 347:JAPIO Nov 1976-2004/May(Updated 040903)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200456
         (c) 2004  Thomson Derwent
```

```
 27/5/3     (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

015996086    **Image available**
WPI Acc No: 2004-153936/200415
Related WPI Acc No: 2000-022990; 2001-182563
XRPX Acc No: N04-122974
  Server computer for financial data transaction in e-commerce, stores data
  packet until computer selected by data processor, is ready to receive
  client packet
Patent Assignee: INTEL CORP (ITLC  )
Inventor: JARDIN C A
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No     Kind   Date     Applicat No     Kind   Date      Week
US 6681327     B1  20040120  US 9854304        A   19980402  200415  B
                             US 99133451       P   19990511
                             US 99345575       A   19990630

Priority Applications (No Type Date): US 99133451 P 19990511; US 9854304 A
  19980402; US 99345575 A 19990630
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
US 6681327    B1    12 H04L-009/00    CIP of application US 9854304
                                      Provisional application US 99133451

Abstract (Basic): US 6681327 B1
        NOVELTY - A data processor connected to a data interface, is
    programmed to access data packet received from the computer, and
    decrypts  the contents of the data packets. The processor selects the
    computer in which the data packet is transmitted. A data storage stores
    the packet until the selected computer is ready to receive client
    packet.
        DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the
    following:
        (1) electronic requests managing system;
        (2) electronic requests managing method;
        (3) communication method; and
        (4) communication system.
        USE - Server computer for data communication and financial data
    transaction in e-commerce application over network such as Internet,
    secure socket layer (SSL) and  Internet   protocol   security   ( IPSec
    ).
        ADVANTAGE - The client session is recovered and completed without
    conveying any of the service difficulties encountered by the entity
    providing service to the client, thus maintaining high customer
    perception of the entity.
        DESCRIPTION OF DRAWING(S) - The figure shows a flowchart explaining
    the server operation.
        pp; 12 DwgNo 4/4
Title Terms: SERVE; COMPUTER; FINANCIAL; DATA; TRANSACTION; STORAGE; DATA;
  PACKET; COMPUTER; SELECT; DATA; PROCESSOR; READY; RECEIVE; CLIENT; PACKET
Derwent Class: T01; W01
International Patent Class (Main):  H04L-009/00
International Patent Class (Additional):  H04L-012/22
File Segment: EPI


 27/5/10     (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014920855
WPI Acc No: 2002-741562/200280
Related WPI Acc No: 2002-741615; 2003-019520; 2003-019527; 2003-313960
XRPX Acc No: N02-584252
```

RAM device has a high-density storage device and a controller to buffer and prioritize incoming access requests into an order maximizing the overlap of the requests' timing cycles

Patent Assignee: LAYER N NETWORKS INC (LAYE-N); LAYER N NETWORKS (LAYE-N); ZSOHAR L (ZSOH-I)

Inventor: BLAKLEY G; DATTA R; MITCHELL O; STEIN K; ZSOHAR L

Number of Countries: 100 Number of Patents: 008

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200288969	A1	20021107	WO 2002US13512	A	20020501	200280	B
US 20020194445	A1	20021219	US 2001288015	P	20010502	200303	
			US 2001300955	P	20010626		
			US 2001300957	P	20010626		
			US 2001326250	P	20011001		
			US 2001326251	P	20011001		
			US 2001326252	P	20011001		
			US 2001326266	P	20011001		
			US 200278253	A	20020216		
US 20030018788	A1	20030123	US 2001300955	P	20010626	200310	
			US 2002180209	A	20020626		
AU 2002254760	A1	20021111	AU 2002254760	A	20020501	200433	
AU 2002256391	A1	20021111	AU 2002256391	A	20020501	200433	
US 6738874	B2	20040518	US 2001288015	P	20010502	200433	
			US 2001300955	P	20010626		
			US 2001300957	P	20010626		
			US 2001326250	P	20011001		
			US 2001326251	P	20011001		
			US 2001326252	P	20011001		
			US 2001326266	P	20011001		
			US 200278253	A	20020216		
US 20040133754	A1	20040708	US 200278253	A	20020216	200445	
			US 2003640462	A	20030813		
US 20040148377	A1	20040729	US 200278253	A	20020216	200450	
			US 2003640499	A	20030813		

Priority Applications (No Type Date): US 200278253 A 20020216; US 2001288015 P 20010502; US 2001300955 P 20010626; US 2001300957 P 20010626 ; US 2001326250 P 20011001; US 2001326251 P 20011001; US 2001326252 P 20011001; US 2001326266 P 20011001; US 2002180209 A 20020626; US 200268294 A 20020205; US 2003640462 A 20030813; US 2003640499 A 20030813

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200288969	A1	E	39	G06F-013/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020194445	A1			G06F-013/28	Provisional application US 2001288015
					Provisional application US 2001300955
					Provisional application US 2001300957
					Provisional application US 2001326250
					Provisional application US 2001326251
					Provisional application US 2001326252
					Provisional application US 2001326266
US 20030018788	A1			G06F-015/16	Provisional application US 2001300955
AU 2002254760	A1			H04L-009/28	Based on patent WO 200289399
AU 2002256391	A1			G06F-013/00	Based on patent WO 200288969
US 6738874	B2			G06F-012/00	Provisional application US 2001288015
					Provisional application US 2001300955
					Provisional application US 2001300957
					Provisional application US 2001326250
					Provisional application US 2001326251

		Provisional application US 2001326252
		Provisional application US 2001326266
US 20040133754 A1	G06F-012/00	Div ex application US 200278253
		Div ex patent US 6738874
US 20040148377 A1	G06F-015/173	Div ex application US 200278253
		Div ex patent US 6738874

Abstract (Basic): WO 200288969 A1

NOVELTY - Buffering access requests by their timing cycles allows low latency access to small blocks of discontinuous data stored in a high density storage device. The buffer may have a number of sections serving different memory banks. The system recognizes when different access requests are directed to different memory banks and prioritizes them to reduce overlap and reduce total access time. Read and write accesses and bank switches can be **grouped** from the buffers.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for

(a) a networking system includes a high density storage device with a controlling prioritizing memory access requests on the basis of their timing cycles

(b) a memory request handling method

(c) and a networking system having network interface devices and network processing engines configured to encrypt and **decrypt** information passing between networking connections and RAM devices with **Internet Protocol Security**

USE - Memory systems for data processing systems.

ADVANTAGE - Uses high-density RAM storage devices to provide low latency access over the full memory address space to small blocks of discontinuous data.

pp; 39 DwgNo 0/4

Title Terms: RAM; DEVICE; HIGH; DENSITY; STORAGE; DEVICE; CONTROL; BUFFER; INCOMING; ACCESS; REQUEST; ORDER; MAXIMISE; OVERLAP; REQUEST; TIME; CYCLE
Derwent Class: T01; W01
International Patent Class (Main): **G06F-012/00 ; G06F-013/00 ; G06F-013/28 ; G06F-015/16 ; G06F-015/173 ; H04L-009/28**
International Patent Class (Additional): **G06F-012/00**
File Segment: EPI

27/5/12 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014822083 **Image available**
WPI Acc No: 2002-642789/200269
XRPX Acc No: N02-508110

Internet protocol (IP) security traffic processing method, involves decrypting **IP security traffic at secondary location to determine its** classification **parameter, if** classification **parameter is not available at primary location**

Patent Assignee: INTEL CORP (ITLC); KUNZE A R (KUNZ-I); STRAHM F W (STRA-I)
Inventor: KUNZE A R; STRAHM F W
Number of Countries: 022 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020104020	A1	20020801	US 2001774429	A	20010130	200269 B
WO 200262033	A2	20020808	WO 2002US2594	A	20020129	200269
EP 1358752	A2	20031105	EP 2002713503	A	20020129	200377
			WO 2002US2594	A	20020129	

Priority Applications (No Type Date): US 2001774429 A 20010130
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020104020	A1		12	G06F-015/173	
WO 200262033	A2	E		H04L-029/00	

Designated States (National): SG
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU

```
   MC NL PT SE TR
EP 1358752     A2 E     H04L-029/06   Based on patent WO 200262033
   Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI
   LU MC NL PT SE TR

Abstract (Basic): US 20020104020 A1
       NOVELTY - The Internet  protocol  security  (IP sec) traffic is
    decrypted  at secondary location to determine its  classification
    parameter, if the  classification  parameter for the IP sec traffic is
    not available at a primary location. The IP sec traffic is forwarded
    based on the determined  classification  parameter.
       DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for:
       (1)  Internet  protocol  security  traffic processing system; and

       (2) Article comprising machine-readable medium storing program for
    processing  Internet  protocol  security  traffic.
       USE - For processing  Internet  protocol  security  (IP sec)
    traffic.
       ADVANTAGE - The traffic is efficiently  classified  and transmitted
    to and/or from the network.
       DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of
    the network configuration.
       pp; 12 DwgNo 2/5
Title Terms: PROTOCOL; IP; SECURE; TRAFFIC; PROCESS; METHOD; IP; SECURE;
  TRAFFIC; SECONDARY; LOCATE; DETERMINE;  CLASSIFY ; PARAMETER;  CLASSIFY ;
  PARAMETER; AVAILABLE; PRIMARY; LOCATE
Derwent Class: T01; W01
International Patent Class (Main):  G06F-015/173 ;  H04L-029/00 ;
  H04L-029/06
International Patent Class (Additional):  H04L-009/00
File Segment: EPI


 27/5/13     (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014796761     **Image available**
WPI Acc No: 2002-617467/200266
XRPX Acc No: N02-488666
  Computer network packet process method, involves performing cryptographic
  process on transferred network packets having high priority by using
  policy
Patent Assignee: GENTY D M (GENT-I); MULLEN S P (MULL-I); VENKATARAMAN G P
  (VENK-I)
Inventor: GENTY D M; MULLEN S P; VENKATARAMAN G P
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
US 20020078341  A1  20020620  US 2000737042    A   20001214  200266  B

Priority Applications (No Type Date): US 2000737042 A 20001214
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 20020078341 A1    10 H04L-009/00

Abstract (Basic): US 20020078341 A1
       NOVELTY - Network packets having high priority are transferred over
    a computer network based on a policy, before the packets having low
    priority. A cryptographic process is performed on the network packets
    using the policy.
       DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for network
    packet management system.
       USE - For applying quality of service policies for computer network
    such as virtual private network.
       ADVANTAGE - Allows the QoS and  IPsec  programs to use the same set
    of priority policies to give identical preferential treatment to high
    priority network packets and overcomes the bandwidth limitations on the
    network. Ensures the high-priority network packets that are not
    significantly slowed down during the encryption/ decryption  process.
        DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of
    the computer network.
        pp; 10 DwgNo 3/4
Title Terms: COMPUTER; NETWORK; PACKET; PROCESS; METHOD; PERFORMANCE;
  CRYPTOGRAPHIC; PROCESS; TRANSFER; NETWORK; PACKET; HIGH; PRIORITY
Derwent Class: T01; W01
International Patent Class (Main):  H04L-009/00
File Segment: EPI


 27/5/14     (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014717339     **Image available**
WPI Acc No: 2002-538043/200257
XRPX Acc No: N02-426073
  Voice over  Internet   protocol   security  module for use in various
  multimedia services such as in telephony to interface between security
  and protocol managers
Patent Assignee: NOKIA CORP (OYNO  ); NUUTINEN M (NUUT-I); NOKIA INC (OYNO
  )
Inventor: NUUTINEN M
Number of Countries: 095  Number of Patents: 004
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
WO 200254704   A2   20020711  WO 2001IB1700    A    20010918  200257  B
US 20020129236  A1   20020912  US 2000752142    A    20001229  200262
EP 1378101     A2   20040107  EP 2001967586    A    20010918  200404
                              WO 2001IB1700    A    20010918
AU 2001287958  A1   20020716  AU 2001287958    A    20010918  200427

Priority Applications (No Type Date): US 2000752142 A 20001229
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
WO 200254704   A2 E  64 H04L-029/06
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
   CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP
   KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT
   RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
   Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
   IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW
US 20020129236 A1       H04L-009/00
EP 1378101     A2 E     H04L-029/06   Based on patent WO 200254704
   Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
   LI LT LU LV MC MK NL PT RO SE SI TR
AU 2001287958 A1       H04L-029/06   Based on patent WO 200254704

Abstract (Basic): WO 200254704 A2
        NOVELTY - The interface between the session initiation protocol
    (SIP) stack and the security manager is called the SIP security
    application interface and provides means to perform all security tasks
    required. The SIP security manager application interface provides means
    for usage of external security services and a SIP security media
    interface provides means for encryption/ decryption  of the media
    stream.
        DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for a SIP
    signaling stack and for a telecommunication system.
        USE - Providing secure voice over Internet protocol terminal.
        ADVANTAGE - Providing authentication and security functions at
    lower level.
        DESCRIPTION OF DRAWING(S) - The drawing shows secure SIP protocol
    stack architecture.
        pp; 64 DwgNo 10/14
```

```
Title Terms: VOICE; PROTOCOL; SECURE; MODULE; VARIOUS; SERVICE; TELEPHONE;
  INTERFACE; SECURE; PROTOCOL
Derwent Class: W01
International Patent Class (Main):  H04L-009/00 ;  H04L-029/06
International Patent Class (Additional): H04M-007/00
File Segment: EPI


 27/5/15     (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014521708     **Image available**
WPI Acc No: 2002-342411/200238
XRPX Acc No: N02-269275
  Data encryption apparatus for private communication over telephone and
  computer network, synchronizes provision of subkey to its respective data
  processing module with passage of data block through data processing
  pipeline
Patent Assignee: AMPHION SEMICONDUCTOR LTD (AMPH-N); MCCANNY J V (MCCA-I);
  MCLOONE M P (MCLO-I)
Inventor: MCCANNY J V; MCLOONE M P
Number of Countries: 027  Number of Patents: 002
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
EP 1191737      A2  20020327  EP 2001122188   A   20010917  200238  B
US 20020041685  A1  20020411  US 2001957314   A   20010919  200238

Priority Applications (No Type Date): GB 200023409 A 20000922
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
EP 1191737    A2 E  18 H04L-009/06
   Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
   LI LT LU LV MC MK NL PT RO SE SI TR
US 20020041685 A1       H04L-009/00

Abstract (Basic): EP 1191737 A2
        NOVELTY - A sub-key skewing module (40) synchronizes the provision
    of each sub-key to its respective data processing module (34) with the
    passage of a data block through the data processing pipeline (32). The
    data block is encrypted or  decrypted  using sub-keys generated from a
    common primary key.
        DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the
    following:
        (a) Data blocks encryption/  decryption  method;
        (b) Computer program product comprising computer usable
    instructions for encrypting or  decrypting  data blocks
        USE - For encrypting data for communication over telephone or
    computer network, also for  IPsec  protocols, ATM cell encryption,
    secure socket layer protocol and access system for terrestrial
    broadcast.
        ADVANTAGE - Increases the processing speed of data encryption/
    decryption  apparatus. Supports the use of different cipher keys in
    consecutive clock cycles and improves the level of security provided by
    the apparatus.
        DESCRIPTION OF DRAWING(S) - The figure shows a schematic view of a
    data encryption apparatus.
        Data Processing pipeline (32)
        Data processing module (34)
        Sub-key skewing module (40)
        pp; 18 DwgNo 3/9
Title Terms: DATA; ENCRYPTION; APPARATUS; PRIVATE; COMMUNICATE; TELEPHONE;
  COMPUTER; NETWORK; SYNCHRONISATION; PROVISION; RESPECTIVE; DATA; PROCESS;
  MODULE; PASSAGE; DATA; BLOCK; THROUGH; DATA; PROCESS; PIPE
Derwent Class: W01
International Patent Class (Main):  H04L-009/00 ;  H04L-009/06
File Segment: EPI
```

```
 27/5/16     (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014481960    **Image available**
WPI Acc No: 2002-302663/200234
XRPX Acc No: N02-236695
  Packet attributes match searching method for database of security rules,
  involves searching suitable static rule and relevant dynamic security
  rules, and applying matching dynamic rules to packet
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC  )
Inventor: ATTWOOD K S; GODWIN J R; OVERBY L H; PERRY B S; WIERBOWSKI D J
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
US 6347376     B1  20020212  US 99373104     A   19990812  200234  B

Priority Applications (No Type Date): US 99373104 A 19990812
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 6347376    B1    21 G06F-011/30

Abstract (Basic): US 6347376 B1
        NOVELTY - The static rule having attributes that match the
    corresponding attributes of the packet is searched and tested to find
    if the static rule contains relevant dynamic security rules. If dynamic
    rules exist, security processing is applied to the packet matching the
    dynamic rules.
        DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the
    following:
        (a) Searching tool for matching values of packet attributes and
    corresponding attribute values associated to each rules;
        (b) Storage medium containing stored executable instructions to
    control computer to search for matching values of packet attributes;
        (c) Computer data signal containing stored executable instructions
    to control computer to search for matching values of packet attributes
        USE - For database of security rules stored in computer network.
        ADVANTAGE - Improves the performance of system  IPsec  rule
    searching. Sets of dynamic rules are partitioned into separate  groups
    such that within a  group  there is no rule order dependence. Thus
    enhances searching.
        DESCRIPTION OF DRAWING(S) - The figure shows the database structure
    arrangement.
        pp; 21 DwgNo 5/13
Title Terms: PACKET; ATTRIBUTE; MATCH; SEARCH; METHOD; DATABASE; SECURE;
  RULE; SEARCH; SUIT; STATIC; RULE; RELEVANT; DYNAMIC; SECURE; RULE; APPLY;
  MATCH; DYNAMIC; RULE; PACKET
Derwent Class: T01; W01
International Patent Class (Main):  G06F-011/30
International Patent Class (Additional):  H04L-009/00
File Segment: EPI


 27/5/17     (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014462031    **Image available**
WPI Acc No: 2002-282734/200233
XRPX Acc No: N02-220851
  Security keys management method for WLAN, involves generating  IPsec
  authentication, encryption and  decryption  keys using certificates and
  private key for packets transferred between mobile terminal and server
Patent Assignee: NOKIA INC (OYNO  )
Inventor: HANSEN H; SALVELA J; STENMAN J
```

```
Number of Countries: 026  Number of Patents: 001
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
EP 1178644      A2  20020206  EP 2001660026    A    20010206  200233  B

Priority Applications (No Type Date): US 2000502567 A 20000211
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
EP 1178644     A2 E  11 H04L-029/06
   Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
   LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): EP 1178644 A2
        NOVELTY - The certificates obtained from a certificate authority
    and a private key are used with Internet key exchange to generate a
    WLAN link level, and the mobile terminal and the access point are
    mutually authenticated. The keys are used to generate  IPsec
    authentication, encryption and  decryption  keys for data packets
    transferred between the mobile terminal and the server.
        USE - For wireless local area network (WLAN).
        ADVANTAGE - The security keys are managed efficiently, preventing
    unauthorized access to the network.
        DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram of
    the IP end-to-end security functions and WLAN link level security.
        pp; 11 DwgNo 3/5
Title Terms: SECURE; KEY; MANAGEMENT; METHOD; GENERATE; AUTHENTICITY;
  ENCRYPTION;  DECRYPTER ; KEY; CERTIFY; PRIVATE; KEY; PACKET; TRANSFER;
  MOBILE; TERMINAL; SERVE
Derwent Class: T01; W01
International Patent Class (Main):  H04L-029/06
International Patent Class (Additional):  H04L-012/24 ;  H04L-012/28
File Segment: EPI


 27/5/18     (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014203019     **Image available**
WPI Acc No: 2002-023716/200203
  Method for producing one chip type ip security based vpn
Patent Assignee: SIGN CO LTD (SIGN-N)
Inventor: KIM M
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
KR 2001066996  A    20010712  KR 200065993     A    20001107  200203  B

Priority Applications (No Type Date): KR 200065993 A 20001107
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
KR 2001066996 A      1 G06F-001/00

Abstract (Basic): KR 2001066996 A
        NOVELTY - A one chip type IP( Internet   Protocol )  security
    based VPN(Virtual private Network) production method is provided to
    produce the IP security function by an ASIC(Application Specific
    Integrated Circuit) for using variously the functions of the VPN.
        DETAILED DESCRIPTION - The method comprises steps of embedding an
    IP security program, defined by an RFC(Requests For Comments), in an
    ASIC, setting a coding/ decoding  algorithm at an external position of
    the ASIC to accept currently used various coding algorithms, and
    producing TCP-IP IO structure for making an Internet access easy. The
    ASIC device can be directly inserted in internal circuit of a
    conventional computer system or be interfaced with the conventional
    computer system.
        pp; 1 DwgNo 1/10
```

```
Title Terms: METHOD; PRODUCE; ONE; CHIP; TYPE; IP; SECURE; BASED
Derwent Class: T01
International Patent Class (Main): G06F-001/00
File Segment: EPI


 27/5/19     (Item 18 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014037772     **Image available**
WPI Acc No: 2001-521985/200157
XRPX Acc No: N01-386874
  Scheme for determining transport level information in the presence of
  Internet  protocol  security encryption using the header to record
  unencrypted information normally included in the payload
Patent Assignee: KOODLI R (KOOD-I); NOKIA CORP (OYNO  ); SENGODAN S
  (SENG-I)
Inventor: KOODLI R; SENGODAN S
Number of Countries: 093  Number of Patents: 005
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
WO 200147169    A2  20010628  WO 2000US34991   A   20001226  200157   B
AU 200132659    A   20010703  AU 200132659     A   20001226  200164
EP 1240766      A2  20020918  EP 2000991431    A   20001226  200269
                              WO 2000US34991   A   20001226
EP 1240766      B1  20030820  EP 2000991431    A   20001226  200356
                              WO 2000US34991   A   20001226
DE 60004707     E   20030925  DE 604707        A   20001226  200371
                              EP 2000991431    A   20001226
                              WO 2000US34991   A   20001226

Priority Applications (No Type Date): US 99471083 A 19991223
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
WO 200147169  A2 E  19 H04L-000/00
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY CA CH
   CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE
   KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU
   SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
   Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
   IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW
AU 200132659  A        H04L-000/00   Based on patent WO 200147169
EP 1240766    A2 E     H04L-029/06   Based on patent WO 200147169
   Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
   LI LT LU LV MC MK NL PT RO SE SI TR
EP 1240766    B1 E     H04L-029/06   Based on patent WO 200147169
   Designated States (Regional): DE FR GB IT
DE 60004707   E        H04L-029/06   Based on patent EP 1240766
                                     Based on patent WO 200147169

Abstract (Basic): WO 200147169 A2
        NOVELTY - A transport payload data unit (106) and an encapsulated
    security payload (ESP) trailer (108) are fully encrypted whereas the
    Internet protocol header (102), the ESP header (104) and the ESP
    authenticator (110) are not encrypted. Some information related to the
    selected information is placed in the security protocol header prior to
    security processing of the packet, so that access can be allowed to
    selected information by intermediate nodes during transmission of the
    packet.
        DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for a method
    of permitting access to selected information in an encrypted packet.
        USE - Determining transport level information in presence of
    Internet  protocol  security encryption.
        ADVANTAGE - No compromise of security.
        DESCRIPTION OF DRAWING(S) - The drawing is a schematic diagram of
    configuration of an Internet protocol packet
```

```
        Payload data unit (106)
        ESP trailer (108)
        Internet protocol header (102)
        ESP header (104)
        pp; 19 DwgNo 1/5
Title Terms: SCHEME; DETERMINE; TRANSPORT; LEVEL; INFORMATION; PRESENCE;
  PROTOCOL; SECURE; ENCRYPTION; HEADER; RECORD; INFORMATION; NORMAL;
  PAYLOAD
Derwent Class: T01; W01
International Patent Class (Main):  H04L-000/00 ;  H04L-029/06
File Segment: EPI


 27/5/20     (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

014037092     **Image available**
WPI Acc No: 2001-521305/200157
Related WPI Acc No: 2001-257355; 2001-521304
XRPX Acc No: N01-386225
  Cryptography acceleration chip has  classification  engine that receives
  complete IP packet and determines specific keys needed to encrypt or
  decrypt  packet
Patent Assignee: BROADCOM CORP (BROA-N)
Inventor: KRISHNA S; LAW P; LIN D; OWEN C; SMITH P; TARDO J; LIN D C; SMITH
  P N; TARDO J J
Number of Countries: 095  Number of Patents: 004
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
WO 200105087   A2  20010118  WO 2000US18617  A   20000707  200157  B
AU 200063425   A   20010130  AU 200063425    A   20000707  200157
EP 1192782     A2  20020403  EP 2000950302   A   20000707  200230
                             WO 2000US18617  A   20000707
US 20030023846  A1  20030130  US 99142870     P   19990708  200311
                             US 99159011     P   19991012
                             US 2000610722   A   20000706
                             US 2002218206   A   20020812

Priority Applications (No Type Date): US 99159011 P 19991012; US 99142870 P
  19990708; US 2000610722 A 20000706; US 2002218206 A 20020812
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
WO 200105087  A2 E  45 H04L-000/00
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
   CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP
   KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT
   RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
   Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
   IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW
AU 200063425  A        H04L-000/00   Based on patent WO 200105087
EP 1192782    A2 E     H04L-029/06   Based on patent WO 200105087
   Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
   LI LT LU LV MC MK NL PT RO SE SI
US 20030023846 A1       H04L-009/00   Provisional application US 99142870

                                     Provisional application US 99159011
                                     Cont of application US 2000610722

Abstract (Basic): WO 200105087 A2
        NOVELTY - The cryptography acceleration chip has a  classification
    engine (204) configured to receive a complete IP packet and determines
    what keys are needed to encrypt or  decrypt  the packet.
        DETAILED DESCRIPTION - The cryptography acceleration chip has a
    classification  engine (204) which determines the keys by parsing
    fields in a header of the IP packet to determine a flow to which the
    packet belongs. The flow has one or more associated keys for encrypting
```

or **decrypting** the packet. The engine supports all necessary modes for **IPSec** security processing. The chip includes internal and external local memories and hash-based look-up table.

USE - For use in cryptography, also incorporated on network line cards or service modules and used in applications as diverse as connecting a single computer to WAN, to large corporate networks, to networks servicing wide geographic areas.

ADVANTAGE - Implements **IPSec** specification at much faster rates than are achievable with current chip designs. Has much reduced local memory requirements.

DESCRIPTION OF DRAWING(S) - The figure shows the high level diagram of cryptography acceleration chip.

Classification engine (204)

pp; 45 DwgNo 2/7

Title Terms: ACCELERATE; CHIP; **CLASSIFY** ; ENGINE; RECEIVE; COMPLETE; IP; PACKET; DETERMINE; SPECIFIC; KEY; NEED; PACKET

Derwent Class: T01; W01

International Patent Class (Main): **H04L-000/00** ; **H04L-009/00** ; **H04L-029/06**

File Segment: EPI

27/5/21 (Item 20 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

014037091 **Image available**

WPI Acc No: 2001-521304/200157

Related WPI Acc No: 2001-257355; 2001-521305

XRPX Acc No: N01-386224

Cryptography acceleration chip used in network line cards, has distributor unit and cryptography engines that are configured to perform parallel cryptographic processing of packets and to maintain packet flow order

Patent Assignee: BROADCOM CORP (BROA-N)

Inventor: KRISHNA S; LAW P; LIN D; OWEN C; TARDO J

Number of Countries: 095 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200105086	A2	20010118	WO 2000US18537	A	20000707	200157	B
AU 200063422	A	20010130	AU 200063422	A	20000707	200157	
EP 1192781	A2	20020403	EP 2000950299	A	20000707	200230	
			WO 2000US18537	A	20000707		

Priority Applications (No Type Date): US 99159011 P 19991012; US 99142870 P 19990708

Patent Details:

```
Patent No  Kind Lan Pg   Main IPC     Filing Notes
WO 200105086  A2 E  45 H04L-000/00
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
   CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP
   KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT
   RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
   Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
   IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW
AU 200063422  A        H04L-000/00   Based on patent WO 200105086
EP 1192781    A2 E     H04L-029/06   Based on patent WO 200105086
   Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
   LI LT LU LV MC MK NL PT RO SE SI
```

Abstract (Basic): WO 200105086 A2

NOVELTY - The distributor unit (206) receives packets and matching **classification** information of the packets and distributes each packet to each of the cryptography processing engines (214). The distributor unit and the engines together enables parallel cryptographic processing of data packets and also maintains packet flow order.

DETAILED DESCRIPTION - The distributor unit inputs the packets to the cryptography engines in round-robin fashion. An order maintenance retirement unit enables the cryptography engines to process incoming packets in out-of-order fashion. INDEPENDENT CLAIMS are also included for the following:

(a) Cryptographic processing accelerating method;
(b) Network communication device

USE - Used in network line cards, web switches, routers or service modules that connect single computer to WAN, to corporate networks to networks servicing wide geographic areas.

ADVANTAGE - Since the chip includes distributor unit and many cryptographic engines, the **IPSec** specification is implemented at much faster rate hence local memory requirements is reduced and need for attached local memory to store packet data or control parameters is avoided.

DESCRIPTION OF DRAWING(S) - The figure shows the high level block diagram of cryptography accelerating chip.

Distributing unit (206)
Cryptographic engines (214)
pp; 45 DwgNo 2/7

Title Terms: ACCELERATE; CHIP; NETWORK; LINE; CARD; DISTRIBUTE; UNIT; ENGINE; CONFIGURATION; PERFORMANCE; PARALLEL; CRYPTOGRAPHIC; PROCESS; PACKET; MAINTAIN; PACKET; FLOW; ORDER
Derwent Class: T01; W01
International Patent Class (Main): **H04L-000/00** ; **H04L-029/06**
File Segment: EPI

27/5/22 (Item 21 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

011745329 **Image available**
WPI Acc No: 1998-162239/199815
Related WPI Acc No: 1998-162043
XRPX Acc No: N98-129124

Regulating flow of messages through firewall having network protocol stack with IP layer - passing decrypted **message up network protocol stack to application level proxy, and determining authentication protocol appropriate for message**

Patent Assignee: SECURE COMPUTING CORP (SECU-N)
Inventor: DE JONGH T; MINEAR S; STOCKWELL E B
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2317792	A	19980401	GB 9719816	A	19970917	199815	B
GB 2317792	B	20010328	GB 9719816	A	19970917	200118	

Priority Applications (No Type Date): US 96715668 A 19960918; US 96715343 A 19960918
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2317792	A		34	H04L-009/00	
GB 2317792	B			H04L-009/00	

Abstract (Basic): GB 2317792 A

The messages flow regulation involves a firewall (18) having a network protocol stack which includes an internet protocol layer. If the message is not encrypted, as determined at the IP layer, it passes the un-encrypted message up the network protocol stack to an application level proxy, while if the message is encrypted, it **decrypts** the message and passes the **decrypted** message up the network protocol stack to the application level proxy.

The **decryption** involves executing a process at the IP layer to **decrypt** the message, passing the **decrypted** message up the network protocol stack to an application level proxy, determining the authentication protocol appropriate for the message, and executing the authentication protocol to authenticate the message sender.

USE - For secure transfer of information between firewalls over unprotected network.

ADVANTAGE - Handles **internet protocol security** or **IPSEC** messages without assuming that encrypted message has access to all services, by controlling service access to individual services within individual network, thus increasing firewall security.

Dwg.1/5

Title Terms: REGULATE; FLOW; MESSAGE; THROUGH; FIREWALL; NETWORK; PROTOCOL; STACK; IP; LAYER; PASS; MESSAGE; UP; NETWORK; PROTOCOL; STACK; APPLY; LEVEL; DETERMINE; AUTHENTICITY; PROTOCOL; APPROPRIATE; MESSAGE

Index Terms/Additional Words: INTERNET; PROTOCOL

Derwent Class: T01; W01

International Patent Class (Main): **H04L-009/00**

File Segment: EPI

```
Set      Items   Description
S1     1456640   ENCRYPT? OR SCRAMBL? OR CIPHER? OR CRYPT? OR CODE? ? OR EN-
              CIPHER? OR CODING OR CODED OR ENCOD?
S2      128104   DECRYPT? OR DESCRAMBL? OR DECIPHER? OR DECOD? OR UNSCRAMBL?
                OR UNENCOD? OR UNENCRYPT? OR UNCOD? OR UNCIPHER?
S3       22659   (PACKET ? OR FRAME? OR DATAGRAM? OR BLOCK()DATA)(2N)(DATA -
              OR INFORMATION)
S4      101027   S1 (2N) (DATA OR INFORMATION)
S5     7151335   CLASSIF? OR CATEGORIZ? OR CATEGORIS? OR CATALOG? OR GROUP?
S6     1048187   PARAMETER? OR DESCRIPT?()ITEM? OR ATTRIBUT? OR (NAME OR ST-
              RUCTURE? OR SIZE OR VALUE)(2N)(DATA OR INFORMATION)
S7       13741   IPSEC OR INTERNET()PROTOCOL()SECURITY
S8      579224   (SECONDARY OR FURTHER OR ADDITIONAL OR NEW OR SUPPLEMENT? -
              OR MORE OR EXTRA?)(2W)(PLACE? OR POSITION? OR LOCATION? OR AR-
              EA? OR SPACE?)
S9      262455   (FIRST OR 1ST OR INITIAL OR LEADING OR CARDINAL OR ORIGINAL
                OR PRIMARY)(2W)(PLACE? OR POSITION? OR LOCATION? OR AREA? OR
              SPACE?)
S10        197   S1 (2N) S3
S11          0   S7 (S) (S2 (2N) S3)
S12        395   S7 (S) S2
S13         22   S7 (S) S3
S14          4   S10 (S) S7
S15         14   S10 (S) S5
S16         20   S10 (S) S2
S17         11   S15 (S) S4
S18         54   S13 OR S14 OR S15 OR S16 OR S17
S19         42   S18 NOT PY>2001
S20         36   S19 NOT PD>20010130
S21         26   RD (unique items)
File  15:ABI/Inform(R) 1971-2004/Sep 06
         (c) 2004 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 647:CMP  Computer Fulltext 1988-2004/Aug W5
         (c) 2004 CMP Media, LLC
File 275:Gale Group Computer DB(TM) 1983-2004/Sep 06
         (c) 2004 The Gale Group
File 674:Computer News Fulltext 1989-2004/Aug W3
         (c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Sep 06
         (c) 2004 The Dialog Corp.
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Sep 06
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Sep 06
         (c) 2004 The Gale Group
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2004/Sep 07
         (c) 2004 PR Newswire Association Inc
File  16:Gale Group PROMT(R) 1990-2004/Sep 06
         (c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 553:Wilson Bus. Abs. FullText 1982-2004/Jul
         (c) 2004 The HW Wilson Co
```

21/5,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

01878240 05-29232
USE FORMAT 9 FOR FULL TEXT
IPSec's double-edged security
Curtis, John
Network World v16n34 PP: 24 Aug 23, 1999 ISSN: 0887-7661 JRNL CODE: NWW
DOC TYPE: Journal article LANGUAGE: English LENGTH: 1 Pages
WORD COUNT: 484

ABSTRACT: A commentary discusses IP Security (IPSec), a virtual private network security technology with integrated support for shared secret key and digital certificate authentication. IPSec also supports encryption with data enfryption standard adn Triple-DES. There is no question that IPSec exceeds the simple authentication and verification of a firewall, providing vendor-independent encryption.

GEOGRAPHIC NAMES: US

DESCRIPTORS: Virtual networks; Private networks; Computer security; Standardization
CLASSIFICATION CODES: 9190 (CN=United States); 5250 (CN=Telecommunications systems); 5140 (CN=Security)

...TEXT: traffic, let alone attempt to intercept application commands and data because all IPSec content is encrypted.

Allowing **IPSec** traffic through a firewall would mean punching a gaping hole in the firewall to allow passage of any traffic that matched only rudimentary **frame** header **information** that merely suggested that it was legitimate **IPSec** traffic. This might weaken overall network security rather than strengthen it.

Instead, the strategy many customers have...

21/5,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

01840979 04-91970
USE FORMAT 9 FOR FULL TEXT
Security an issue when considering frame relay
Canavan, John
Telecommunications (Americas Edition) v33n6 PP: 75 Jun 1999 CODEN: TLCOAY ISSN: 0278-4831 JRNL CODE: TEC
DOC TYPE: Journal article LANGUAGE: English LENGTH: 1 Pages
WORD COUNT: 977

ABSTRACT: Security is often an issue with frame relay because frame relay switches data over shared lines that are frequently not owned or managed by the service provider with whom the customer has contracted. While private networks utilizing frame relay may be safer than sending data over an insecure network such as the Internet, do not assume that there are not risks. When selecting a frame relay service provider, a company should discuss physical security issues with all potential vendors. Keep in mind that frame relay can use in-band and out-of-band channels. The different security features of permanent virtual circuits and switched virtual circuits are discussed.

GEOGRAPHIC NAMES: US
DESCRIPTORS: Network security; Frame relay; Technological planning; Network switching
CLASSIFICATION CODES: 5250 (CN=Telecommunications systems); 9190 (CN=United

States); 5140 (CN=Security)

...TEXT: service providers who can provide end-to-end private network connectivity; steps need to be taken to **encrypt information** . **Encryption** with **frame** relay is more complicated than with other protocols, such as IP Frame relay operates at a lower...

...to-point connections. As a result, if you encrypt the entire frame relay packet, it must be **decrypted** by the data link layer recipient to determine how to forward the packet. The packet has to be **decrypted** and reencrypted for each point-to-point hop along the data link layer. This requires an entire...

21/5,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01648562 02-99551
USE FORMAT 9 FOR FULL TEXT
The LAN in the WAN: Part II
Sullebarger, Bob
Communications News v35n6 PP: 56-57 Jun 1998 ISSN: 0010-3632
JRNL CODE: CNE
DOC TYPE: Journal article LANGUAGE: English LENGTH: 2 Pages
WORD COUNT: 1148

ABSTRACT: In contrast to frame relay, IP is a connectionless technology. In today's WAN, IP is a best effort service; performance and delay may vary greatly with traffic conditions inside the WAN. The appeal of IP is in its ubiquity. An IP flow may hope across mutliple disparate Layer2 networks to reach its destination without requiring any fundamental protocol conversion. Frame relay, asynchronous transfer mode and point-to-point protocol networks can all transport IP with no difficulty, and IP is rapidly becoming a common underlying transport protocol for most applications. There are 2 basic types of IP-VPNs: 1. those built over the public Internet using tunneling technologies like L2TP, L2F and point-to-point tunnel protocol, and 2. those built on top of carrier-class public networks based on multiprotocol label switching, an emerging IP switching technology being defined by the Internet Engineering Task Force. Network service providers find MPLS-based IP-VPNs attractive because the service is straightforward to market to customers.

GEOGRAPHIC NAMES: US

DESCRIPTORS: Private networks; Virtual networks; Technological planning; Systems management; Internet Protocol
CLASSIFICATION CODES: 5250 (CN=Telecommunications systems); 9190 (CN=United States)

...TEXT: be resolved if IP is to become an effective option for applications that are today supported by **frame** relay **data** services. Security issues are now being addressed via encryption and authentication schemes such as **IPSec** , and by tunneling technologies such as Layer 2 tunneling protocol (L2TP).

While the resource reservation protocol (RSVP...

21/5,K/8 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01704672 SUPPLIER NUMBER: 15066868 (USE FORMAT 7 OR 9 FOR FULL TEXT)
New PA-RISC processor decodes MPEG video; HP's PA-7100LC uses new instructions to eliminate decoder chip. (Moving Pictures Experts Group standard) (includes related article on servers based on the PA-7100LC)

(Product Announcement)
Gwennap, Linley
Microprocessor Report, v8, n1, p16(2)
Jan 24, 1994
DOCUMENT TYPE: Product Announcement ISSN: 0899-9341 LANGUAGE:
ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1839 LINE COUNT: 00143

COMPANY NAMES: Hewlett-Packard Co.--Product introduction
DESCRIPTORS: Microprocessor; Product Introduction
PRODUCT/INDUSTRY NAMES: 3674124 (Microprocessor Chips)
SIC CODES: 3571 Electronic computers; 3577 Computer peripheral equipment, not elsewhere classified; 3674 Semiconductors and related devices
TICKER SYMBOLS: HWP
TRADE NAMES: HP PA-RISC PA-7100LC (Microprocessor)--Product introduction
FILE SEGMENT: CD File 275

... instructions, the new variants are available in signed and unsigned versions. Signed arithmetic is frequently used when **deciphering** MPEG "P" and "B" **frames** , which **encode** **data** as the signed difference between the current frame and one or two others.

The new instructions all...

21/5,K/10 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01506108 SUPPLIER NUMBER: 11983136 (USE FORMAT 7 OR 9 FOR FULL TEXT)
MPEG: the gory details. (The Moving Pictures Experts Group **standard defines three types of** frame information : **intra-** coded frame , **Predictive frame and Bidirectional-interpolation)**
Dyson, Peter
Digital Media, v1, n9, p21(1)
Feb 17, 1992
ISSN: 1056-7038 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 665 LINE COUNT: 00048

SPECIAL FEATURES: illustration; chart
DESCRIPTORS: Video Display; Standard; Analysis; Motion Pictures; Pixels; Huffman Code; Technology
FILE SEGMENT: CD File 275

MPEG: the gory details. (The Moving Pictures Experts Group **standard defines three types of** frame information : **intra-** coded frame , **Predictive frame and Bidirectional-interpolation)**

21/5,K/23 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06308883 Supplier Number: 54527482 (USE FORMAT 7 FOR FULLTEXT)
DVD-Audio to get content protection.
TRASK, SIMON
Pro Sound News Europe, v14, n4, p26(1)
April, 1999
ISSN: 0269-4735
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 181
PUBLISHER NAME: Spotlight Publications
COMPANY NAMES: *International Business Machines Corp.; Intel Corp.; Panasonic Corp.; Toshiba Corp.
EVENT NAMES: *389 (Alliances, partnerships); 350 (Product standards, safety, & recalls)
GEOGRAPHIC NAMES: *1USA (United States); 9JAPA (Japan)

PRODUCT NAMES: *3573217 (Optical Disk Drives); 7372691 (Data Encryption Software)
INDUSTRY NAMES: ARTS (Arts and Entertainment); BUSN (Any type of business); INTL (Business, International)
NAICS CODES: 334112 (Computer Storage Device Manufacturing); 51121 (Software Publishers)
SPECIAL FEATURES: COMPANY

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...companies have now approved a content-protection framework devised by IBM, Intel, Panasonic and Toshiba that uses **encryption** to **scramble data** . The new **framework** will allow content owners to set various levels of copy protection for their discs, ranging from a...

...IBM's program director of digital media standards and co-chairman of the Copy Protection Technical Working **Group** : "In order to encourage the music companies to put their music on DVD-Audio, we had to...

21/5,K/24 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

03776203 Supplier Number: 45369940 (USE FORMAT 7 FOR FULLTEXT)
Bitstream Integrity
One to One, p77
March, 1995
ISSN: 0268-8786
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1476
PUBLISHER NAME: Miller Freeman UK Ltd.
EVENT NAMES: *350 (Product standards, safety, & recalls)
GEOGRAPHIC NAMES: *4EUUK (United Kingdom)
PRODUCT NAMES: *3573220 (Computer Memory Units)
INDUSTRY NAMES: ARTS (Arts and Entertainment); BUSN (Any type of business); INTL (Business, International)
NAICS CODES: 334413 (Semiconductor and Related Device Manufacturing)

... as I3 and I11).See Fig7.
To provide timing information, the CD frames are organised into a **group** of 98 **frames** . The **information** is **encoded** in eight channels corresponding to P, Q, R, S, T, U, V, and W. Currently the P...

21/5,K/25 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

03032006 Supplier Number: 44120111 (USE FORMAT 7 FOR FULLTEXT)
VOICE-OVER-DATA COMES ACROSS LOUD AND CLEAR
Electronic Engineering Times, p61
Sept 27, 1993
ISSN: 0192-1541
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1361
PUBLISHER NAME: CMP Publications, Inc.
EVENT NAMES: *220 (Strategy & planning)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *4800000 (Telecommunication Services)
INDUSTRY NAMES: BUSN (Any type of business); ELEC (Electronics); ENG (Engineering and Manufacturing)
NAICS CODES: 513 (Broadcasting and Telecommunications)
SPECIAL FEATURES: INDUSTRY

... time a retransmit command from the receiving modem controller reaches the transmitting modem controller, the time to **decode** the speech segment containing the error may have already passed. Thus, a special protocol is required which...
...was in error while continuing to send new frames of the 4,800-bits/s ASM-CELP **encoded** speech **data** . The speech **frame** containing errors is used as received; however, it should be pointed out that errors occurring in the...

```
Set     Items   Description
S1     813617   ENCRYPT? OR SCRAMBL? OR CIPHER? OR CRYPT? OR CODE? ? OR EN-
             CIPHER? OR CODING OR CODED OR ENCOD?
S2      89240   DECRYPT? OR DESCRAMBL? OR DECIPHER? OR DECOD? OR UNSCRAMBL?
              OR UNENCOD? OR UNENCRYPT? OR UNCOD? OR UNCIPHER?
S3      17745   (PACKET ? OR FRAME? OR DATAGRAM? OR BLOCK()DATA)(2N)(DATA -
             OR INFORMATION)
S4      50661   S1 (2N) (DATA OR INFORMATION)
S5    2602862   CLASSIF? OR CATEGORIZ? OR CATEGORIS? OR CATALOG? OR GROUP?
S6    2264167   PARAMETER? OR DESCRIPT?()ITEM? OR ATTRIBUT? OR (NAME OR ST-
             RUCTURE? OR SIZE OR VALUE)(2N)(DATA OR INFORMATION)
S7       1302   IPSEC OR INTERNET()PROTOCOL()SECURITY
S8      56228   (SECONDARY OR FURTHER OR ADDITIONAL OR NEW OR SUPPLEMENT? -
             OR MORE OR EXTRA?)(2W)(PLACE? OR POSITION? OR LOCATION? OR AR-
             EA? OR SPACE?)
S9      30351   (FIRST OR 1ST OR INITIAL OR LEADING OR CARDINAL OR ORIGINAL
              OR PRIMARY)(2W)(PLACE? OR POSITION? OR LOCATION? OR AREA? OR
             SPACE?)
S10       349   S1 (2N) S3
S11         0   S7 AND (S2 (2N) S3)
S12        40   S7 AND S2
S13        23   S7 AND S3
S14         8   S10 AND S7
S15        40   S10 AND S5
S16        85   S10 AND S2
S17        85   S16 AND S3
S18         1   S17 AND S7
S19       101   S12 OR S13 OR S14 OR S15 OR S18
S20        55   S19 NOT PY>2001
S21        55   S20 NOT PD?20010130
S22        51   RD (unique items)
File   8:Ei Compendex(R) 1970-2004/Aug W5
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/Aug
         (c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/Jul 12
         (c) 2004 EBSCO Publishing
File  65:Inside Conferences 1993-2004/Sep W1
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Aug W5
         (c) 2004 Institution of Electrical Engineers
File 256:TecInfoSource 82-2004/Jul
         (c)2004 Info.Sources Inc
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File  94:JICST-EPlus 1985-2004/Aug W2
         (c)2004 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Jul
         (c) 2004 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2004/Jun W1
         (c) 2004 FIZ TECHNIK
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
```

22/5/2   (Item 2 from file: 8)
DIALOG(R)File   8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

06013011   E.I. No: EIP02096873388
Title: Securing IP networking architectures
Author: Paridaens, Olivier; Gamm, Bernhard; Howard, Brett
Corporate Source: Alcatel Corp. CTO Net. Strat. Group, Antwerp, Belgium
Source: Alcatel Telecommunications Review n 2 2001. p 122-128
Publication Year: 2001
CODEN: ATREFX   ISSN: 1267-7167
Language: English
Document Type: JA; (Journal Article)   Treatment: T; (Theoretical)
Journal Announcement: 0203W1

Abstract: Security mechanisms for Internet protocol (IP) networking architectures to cope with potential security threats in IP-based environments were presented. The security features of IP security service such as data integrity check, data authentication, traffic flow confidentiality and replay prevention were also discussed. The IP security system can be used to secure any type of traffic carried over IP, as it is applied at the IP level. (Edited abstract)

Descriptors: Network protocols; Security of **data** ; Telecommunication traffic; **Packet networks** ; **Data** communication systems; **Cryptography** ; Database systems; Client server computer systems; Algorithms

Identifiers: **Internet protocol security** ; Internet protocol packets

Classification Codes:
723.2 (Data Processing); 721.1 (Computer Theory (Includes Formal Logic, Automata Theory, Switching Theory & Programming Theory)); 723.3 (Database Systems); 722.4 (Digital Computers & Systems)
723 (Computer Software, Data Handling & Applications); 716 (Electronic Equipment, Radar, Radio & Television); 721 (Computer Circuits & Logic Elements); 722 (Computer Hardware)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATION ENGINEERING)

22/5/3   (Item 3 from file: 8)
DIALOG(R)File   8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

05851362   E.I. No: EIP01286573817
Title: Multiple description coding using exact discrete radon transform
Author: Parrein, B.; Normand, N.; Guedon, J.P.
Corporate Source: IRCCyN UMR 6597 Image Video Communication team EPUN, 50609-44306 Nantes Cedex 3, France
Conference Title: Data Compression Conference
Conference Location: Snowbird, UT, United States   Conference Date: 20010327-20010329
Sponsor: Brandeis University
E.I. Conference No.: 58224
Source: Data Compression Conference Proceedings 2001. p 508
Publication Year: 2001
CODEN: DDCCF9   ISSN: 1068-0314
Language: English
Document Type: CA; (Conference Article)   Treatment: T; (Theoretical); X; (Experimental)
Journal Announcement: 0107W2

Abstract: A balanced multiple description coding is proposed. With a complete adequation between projections and packets, this Priority Encoding Transmission (PET) system can be used over packet switch data networks as the Internet without scalability management. (Edited abstract)

Descriptors: *Image coding; Mathematical transformations; Computational methods; Numerical methods; Color image processing; Encoding (symbols); Packet networks; Switching networks; Internet; Management information systems; Image compression

Identifiers: Multiple description coding; Discrete Radon transform; Layered coding; Numerical shape pixel; Mojette transform; Priority

encoding transmission; **Packet switch data network ; Join** t photographic experts **group** ; Motion pictures experts **group**
Classification Codes:
723.2 (Data Processing); 921.3 (Mathematical Transformations); 921.6 (Numerical Methods); 723.5 (Computer Applications)
723 (Computer Software, Data Handling & Applications); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

22/5/4 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05846001 E.I. No: EIP01276564820
Title: Packet loss resilient, scalable audio compression and streaming for IP networks
Author: Leslie, B.; Sandler, M.
Conference Title: 2nd International Conference on 3G Mobile Communication Technology
Conference Location: London, United Kingdom Conference Date: 20010326-20010328
E.I. Conference No.: 58158
Source: IEE Conference Publication n 477 2001. p 119-123
Publication Year: 2001
CODEN: IECPB4 ISSN: 0537-9989
Language: English
Document Type: CA; (Conference Article) Treatment: A; (Applications); T ; (Theoretical); X; (Experimental)
Journal Announcement: 0107W1
Abstract: Current popular internet audio streaming solutions impose a division between source coding (provided, for example, by MPEG Layer III-MP3) and channel coding, which is accomplished in the server, typically by means of packet retransmission. We present a novel joint source and channel coder which provides packet loss recovery and continuous bitrate scalability. These functionalities are well suited to streaming audio over 3rd and future generation wireless broadband networks. 13 Refs.
Descriptors: Mobile telecommunication systems; Network protocols; Internet; Voice/ **data** communication systems; **Packet networks** ; Signal **encoding** ; Image compression; Communication channels (information theory); Wireless telecommunication systems; Broadband networks
Identifiers: Packet loss; Scalable audio compression; Scalable audio streaming; Internet protocol; Motion pictures experts **group** ; Source coding; Channel coding; Third generation networks
Classification Codes:
716.1 (Information & Communication Theory); 723.5 (Computer Applications); 716.3 (Radio Systems & Equipment); 723.2 (Data Processing)
716 (Electronic Equipment, Radar, Radio & Television); 723 (Computer Software, Data Handling & Applications)
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 72 (COMPUTERS & DATA PROCESSING)

22/5/5 (Item 5 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05733229 E.I. No: EIP00125435552
Title: Network security (security in large networks)
Author: Singh, Manjinder; Singh, Sarabjit
Corporate Source: Panjab Univ, Chandigarh, India
Conference Title: 25th Annual IEEE Conference on Computer Network (LCN 2000)
Conference Location: Tampa, FL, USA Conference Date: 20001108-20001110
Sponsor: IEEE Computer Society
E.I. Conference No.: 57705
Source: Conference on Local Computer Networks 2000. IEEE, Piscataway, NJ,

USA. p 88-93

Publication Year: 2000

CODEN: CLCPDN ISSN: 0742-1303

Language: English

Document Type: CA; (Conference Article) Treatment: T; (Theoretical)

Journal Announcement: 0101W4

Abstract: It is common that users or hosts in a large network are partitioned and organized as a hierarchical tree where children of the same parent from a **group** . Secure broadcasting intends to provide a secure communication channel from a sending principal to a **group** of legal receiving principals. Only legal receiving principals can decrypt the message, and illegal receiving principals cannot acquire any information from the broad casted message. In this paper, we propose a secure broadcasting protocol in which only one packet is transmitted for every broadcast, and the size of the broadcasted packet is small. (Author abstract) 10 Refs.

Descriptors: Computer networks; Security of data; Communication channels (**information** theory); **Packet switching** ; Broadcasting; **Cryptography** ; Network protocols

Identifiers: Network security

Classification Codes:

723.2 (Data Processing); 716.1 (Information & Communication Theory)

716 (Radar, Radio & TV Electronic Equipment); 718 (Telephone & Line Communications); 723 (Computer Software)

71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING)

22/5/6 (Item 6 from file: 8)

DIALOG(R)File 8:Ei Compendex(R)

05644709 E.I. No: EIP00095307475

Title: Uplink packet access control in WCDMA

Author: Wiberg, Niclas; Gioia, Antonella

Corporate Source: Ericsson Radio Systems AB, Linkoping, Sweden

Conference Title: VTC2000: 51st Vehicular Technology Conference 'Shaping History Through Mobile Technologies'

Conference Location: Tokyo, Jpn Conference Date: 19000515-19000518

E.I. Conference No.: 57188

Source: IEEE Vehicular Technology Conference v 3 2000. IEEE, Piscataway, NJ, USA. p 2203-2206

Publication Year: 2000

CODEN: IVTCDZ ISSN: 0740-0551

Language: English

Document Type: CA; (Conference Article) Treatment: T; (Theoretical)

Journal Announcement: 0010W2

Abstract: Three different access control algorithms for uplink packet transmission in a WCDMA system are investigated and compared. The first two methods, based on the number of channels and on the received interference, respectively, have appeared before in the literature. The third method is new and operates on cell **group** level, i.e. it is centralized. The methods are compared regarding achieved system throughput and the ability to control the uplink interference. The centralized method is found to be superior to the other algorithms, and as an added benefit it does not require interference measurements. (Author abstract) 4 Refs.

Descriptors: Cellular radio systems; Telecommunication control; **Packet switching** ; **Data** communication systems; **Code** division multiple access; Radio links; Communication channels (information theory); Radio interference; Algorithms; Spurious signal noise

Identifiers: Uplink packet access control; Interference measurement; Uplink interference

Classification Codes:

716.3 (Radio Systems & Equipment); 722.3 (Data Communication, Equipment & Techniques); 716.1 (Information & Communication Theory)

716 (Radar, Radio & TV Electronic Equipment); 722 (Computer Hardware)

71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING)

22/5/16 (Item 16 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

04902266 E.I. No: EIP98013999583
Title: Bulletproof IP
Author: Thayer, Rodney
Corporate Source: Sable Technology Corp, Boston, MA, USA
Source: Data Communications v 26 n 16 Nov 21 1997. p 54-58, 60
Publication Year: 1997
CODEN: DACODM ISSN: 0363-6399
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 9803W1

Abstract: The Internet Engineering Task Force is adding some armor for the Internet protocol (IP) security. The **IPSec** suite of security protocols make provisions for authentication and encryption that make the data transversing Internet a lot safer. These protocols fall into three categories: encapsulating security payload (ESP) and authentication header (AH) which define encryption and authentication methods for IP payloads; and the IP security association key management protocol (ISAKMP) which manages the exchange of secret keys between senders and receivers of ESP or AH packets. **IPSec** 's authentication feature guard against attacks launched from inside or outside the network while encryption keep hackers from **decoding** packets as they traverse the link.

Descriptors: Security of data; Network protocols; Cryptography; Wide area networks; Local area networks; **Codes** (symbols); **Packet switching ; Information** services; Data communication systems; Gateways (computer networks)

Identifiers: Internet protocol (IP); Transport control protocol (TCP); Encapsulating security payloads (ESP); Authentication headers (AH)

Classification Codes:
723.2 (Data Processing); 722.3 (Data Communication, Equipment & Techniques); 903.4 (Information Services)
723 (Computer Software); 722 (Computer Hardware); 716 (Radar, Radio & TV Electronic Equipment); 903 (Information Science)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS); 90 (GENERAL ENGINEERING)

22/5/17 (Item 17 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

04608567 E.I. No: EIP97013502455
Title: Segmented image coding with contour simplification for video sequences
Author: Christopoulos, V.A.; Christopoulos, C.A.; Philips, W.; Cornelis, J.
Corporate Source: Vrije Universiteit Brussel, Brussels, Belgium
Conference Title: Proceedings of the 1996 IEEE International Conference on Image Processing, ICIP'96. Part 1 (of 3)
Conference Location: Lausanne, Switz Conference Date: 19960916-19960919
Sponsor: IEEE
E.I. Conference No.: 45905
Source: IEEE International Conference on Image Processing v 1 1996. IEEE, Los Alamitos, CA, USA,96CH35919. p 693-696
Publication Year: 1996
CODEN: 85QTAW
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 9703W3

Abstract: In this paper a segmented image coding algorithm for video sequences is presented. The first **frame** in the **data** is always **encoded** in intraframe mode, while the rest of the **frames** in the **data** are **encoded** in interframe mode. The interframe encoding is based on (1) block motion vector estimation and coding, (2) segmentation of the prediction error image and **classification** of the regions in foreground/background, (3) contour simplification and coding, and (4) texture approximation by a linear combination of weakly separable base functions and coefficient coding. The contour simplification leads to an average reduction of 30% in the number of bits needed for the contour coding, the system can be adjusted at different bitrates by parameter tuning, the simulation results are of high quality in terms of PSNR and show that our coding approach is particularly promising for very low bitrate applications. (Author abstract) 13 Refs.

Descriptors: *Image coding; Image segmentation; Algorithms; Error compensation; Computer simulation; Signal to noise ratio; Image quality; Parameter estimation; Image compression

Identifiers: Interframe coding; Video sequences contour simplification

Classification Codes:

723.2 (Data Processing); 741.1 (Light/Optics); 721.1 (Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory); 723.5 (Computer Applications)

741 (Optics & Optical Devices); 723 (Computer Software); 721 (Computer Circuits & Logic Elements)

74 (OPTICAL TECHNOLOGY); 72 (COMPUTERS & DATA PROCESSING)

22/5/21 (Item 1 from file: 2)

DIALOG(R)File 2:INSPEC

7204226 INSPEC Abstract Number: B2002-04-6210L-112, C2002-04-6130S-024

Title: IPSec **/PHIL (packet header information list): design, implementation, and evaluation**

Author(s): Chien-Lung Wu; Wu, S.F.; Narayan, R.

Author Affiliation: North Carolina State Univ., Raleigh, NC, USA

Conference Title: Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No.01EX495) p.206-11

Editor(s): Li, J.; Luijten, R.; Park, E.K.

Publisher: IEEE, Piscataway, NJ, USA

Publication Date: 2001 Country of Publication: USA xx+608 pp.

ISBN: 0 7803 7128 3 Material Identity Number: XX-2001-02344

U.S. Copyright Clearance Center Code: 0-7803-7128-3/01/$10.00

Conference Title: Proceedings Tenth International Conference on Computer Communications and Networks

Conference Sponsor: Army Res. Lab.; IBM; Telcordia; Norkia; Avaya; IEEE Commun. Soc

Conference Date: 15-17 Oct. 2001 Conference Location: Scottsdale, AZ, USA

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P); Experimental (X)

Abstract: For most TCP/UDP/IP applications, when a packet or a message arrives, usually only the payload portion of the original packet can be obtained by the application. For instance, if a packet has been delivered through some **IPSec** (IP security) tunnels along the route path, then the application, in general, does not know exactly which tunnels have been used to deliver this particular packet. The **IPSec** /PHIL (packet header information list) interface has been designed and implemented such that an "authorized" application is able to know which set of **IPSec** tunnels has been used to deliver a particular incoming packet. Furthermore, **IPSec** /PHIL enables controllability over which set of **IPSec** tunnels is used to send a particular outgoing packet. **IPSec** /PHIL is a key component in the Deciduous decentralized source tracing system to correlate the **IPSec** information with intrusion detection results. Other **IPSec** /PHIL applications we have built include a SNMPv3 security module using **IPSec** as well as an **IPSec** tunnel switching router. (17 Refs)

Subfile: B C

Descriptors: Internet; protocols; security of data; telecommunication security

Identifiers: IP security; **IPSec** protocol suite; **packet header information list** ; **TCP|UDP|IP|** ; UDP; IP; **IPSec** tunnels; Deciduous;

decentralized source tracing system; intrusion detection results; SNMPv3 security module; tunnel switching router
Class Codes: B6210L (Computer communications); B6150M (Protocols); C6130S (Data security); C5640 (Protocols); C5620W (Other computer networks)
Copyright 2002, IEE

22/5/22 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

7109526 INSPEC Abstract Number: C2002-01-6130S-073
Title: Accelerating high-speed encryption: one bottleneck after another
Author(s): Cravotta, N.
Journal: EDN (US Edition) vol.46, no.18 p.38-40, 42, 44, 46, 48
Publisher: Cahners Publishing,
Publication Date: 16 Aug. 2001 Country of Publication: USA
CODEN: EDNEFD ISSN: 0012-7515
SICI: 0012-7515(20010816)46:18L.38:AHSE;1-P
Material Identity Number: G340-2001-017
Language: English Document Type: Journal Paper (JP)
Treatment: General, Review (G)

Abstract: The challenge of accelerating cryptographic functions, such as encryption and **decryption** , at high data rates is no longer limited to speeding algorithm processing. Establishing and managing secure sessions, either using SSL or **IPSec** , requires complex handshaking that is processor-intensive, At higher data rates, there comes a point when a server can no longer feed an accelerator because the server's ability to process packets becomes the bottleneck. To achieve higher performance, accelerators have to offload more than just the encryption algorithms. Managing SSL and **IPSec** -that is, getting data out of the packet, then putting it back in-has become a larger part of the security problem. The trick is designing a system in which you eliminate bottlenecks, not just move them. (0 Refs)

Subfile: C
Descriptors: electronic commerce; message authentication; public key cryptography; system buses; transport protocols
Identifiers: high-speed encryption; cryptographic function acceleration; encryption; **decryption** ; high data rates; algorithm bottleneck; secure sessions; SSL; **IPSec** ; complex handshaking; VPN; hashing; secure socket layer; backplane bottleneck
Class Codes: C6130S (Data security); C5640 (Protocols); C5610S (System buses); C6130E (Data interchange)
Copyright 2001, IEE

22/5/30 (Item 4 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00126665 DOCUMENT TYPE: Review

PRODUCT NAMES: Encryption (832022); PKI (838896)

TITLE: Cryptography: Lock and Key For a Safer Net
AUTHOR: Fratto, Mike
SOURCE: Network Computing, v11 n20 p83(2) Oct 16, 2000
ISSN: 1046-4468
HOMEPAGE: http://www.NetworkComputing.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Cryptography ensures private data transmission over public networks. In a public key encryption system, messages are encrypted with publicly available keys, but **decryption** requires a unique secret key held by the intended recipient. Public-key cryptography was invented by the founders of RSA Security, and early users were AT&T, Lotus Development, Microsoft, and WordPerfect, which used the technology to add security to their applications. For Internet transmission, public key encryption is widely used. Multiple agencies process distribution of key pairs. Standards such as **IPSec** create a relatively interoperable environment for security implementation. However, the U.S. government has effectively restricted broad-based adoption of public key infrastructure (PKI), since the U.S. has limited the length of encryption keys, although the most difficult-to-crack messages have the longest encryption keys. Because the Internet requires the ability to deploy encrypted messages to and from all connected desktops, Secure Sockets Layer (SSL) was developed as a simple, scalable solution that uses a unique cryptographic key for each session. In the mid 1990s, virtual private networks (VPNs), which encrypt all data sent between hosts or networks, emerged to provide secure transmission.

COMPANY NAME: Vendor Independent (999999)
DESCRIPTORS: Communications Standards; Computer Security; Encryption;
Government Regulations
REVISION DATE: 20010228

22/5/31 (Item 5 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00125001 DOCUMENT TYPE: Review

PRODUCT NAMES: VPNs (837253)

TITLE: VPNs Come Of Age
AUTHOR: Seltzer, Larry
SOURCE: Internet World, p34(3) Aug 15, 2000
ISSN: 1097-8291
HOMEPAGE: http://www.iw.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Virtual private networks (VPNs) transport packets 'for your network connection that are are packaged as data on the Internet, transported to the network to which you want to connect, and opened up and released onto that network once again as real packets.' Network data is encrypted before it is sent over the Internet and **decrypted** at the receiving end. Remote access VPN technology is older than VPN technology in which complete LANs are connected via the Internet. The latter method is effective for providing business partners with restricted access to a company network and to connect branch offices via the network, instead of through high-cost leased lines. For instance, DST Innovis specializes in emerging markets, for which DST Innovis provides data center and networking services. Microsoft and 3Com support Point-to-Point Tunneling Protocol (PPTP), a standard method for tunneling one protocol inside another. Microsoft provides free clients for Windows95 and Windows NT 4 Workstation, and server components in Windows NT 4 Server. A large third-party VPN market currently thrives, however, and Microsoft and Cisco Systems recently developed Layer 2 Tunneling Protocol (L2TP), which is the next generation of PPTP. Microsoft supports L2TP and **IPSec** in Windows 2000; **IPSec** is becoming the standard for VPNs and is supported in most up-to-date products. Firewall and encryption card vendors, including Check Point and IRE, also provide VPNs.

COMPANY NAME: Vendor Independent (999999)
DESCRIPTORS: Computer Security; Internet Security; Internetworking;
Network Administration; Network Software; System Monitoring; VPNs
REVISION DATE: 20020630

22/5/32 (Item 6 from file: 256)
DIALOG(R)File 256:TecInfoSource

00124276 DOCUMENT TYPE: Review

PRODUCT NAMES: IPSec **(836796); PKI (838896**

TITLE: PKI provides the foundation for end-to-end Internet security
AUTHOR: Staff
SOURCE: Government Computer News, v19 n5 p51(2) Mar 6, 2000
ISSN: 0738-4300
HOMEPAGE: http://www.gcn.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Although the **IPSec** protocol is good protection, it is not perfect because it does not scale effectively beyond virtual private networks (VPNs) to the enterprise. **IPSec** uses the Internet Key Exchange Protocol, which deploys unique keys to manage each node in the network. Therefore, the numbers of keys required increases almost out of control as new nodes are added, which exponentially increases management workload. Lack of interoperability among various vendors products is also an issue, and **IPSec** can clog encrypted network traffic unacceptably. However, **IPSec** is supported by most larger vendors. Public key infrastructure (PKI) is an emerging and developing set of standards for encryption, authentication, and validation of network transactions through use of digital certificates and certification authorities. The government is directly engaged in testing and use of PKI technology in the Healthcare Internet Interoperability Pilot, which authenticates users and tracks support and expenditures for 500,000 people at hospitals, government agencies, and insurance companies. The Fed also has its own PKI pilot program, the Federal Public-Key Infrastructure Project. With PKI, users get two separate keys (public and private). Message senders use the recipient's public key, which is like an address; the receiver **decrypts** with the private key. PKI can be costly and difficult to deploy and requires a central directory for storage of digital certificates and other data.

COMPANY NAME: Vendor Independent (999999)
DESCRIPTORS: Communications Standards; Computer Security; Encryption; Firewalls; Government; Internet Security; Internetworking; System Monitoring
REVISION DATE: 20011030

22/5/33 (Item 7 from file: 256)
DIALOG(R)File 256:TecInfoSource

00118979 DOCUMENT TYPE: Review

PRODUCT NAMES: VPNs (837253)

TITLE: VPNs are easy--once you get the clients installed
AUTHOR: Greene, Tim
SOURCE: Network World, v16 n22 p28(1) May 31, 1999
ISSN: 0887-7661
HOMEPAGE: http://www.nwfusion.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

A discussion is provided of distribution, installation, and maintenance of virtual private network (VPN) clients. For some VPNs, thousands of users have to be supplied with clients, which can be a daunting task, since the numberof end-users linked is directly proportional to the amount of remote client software required. VPN vendors are tackling the problem. For instance, many make clients available as Web downloads, and include wizards that guide end-users through installation and also update software as users log on to a corporate network. Increasing numbers of companies have begun to use VPNs, which use the Internet as a WAN connection for remote access. The most straightforward client available is one already distributed with OSs used by the remote PCs. For instance, Windows 9x/NT all support VPN tunneling technology based on Point to Point Tunneling Protocol (PPTP). However, for users who are not satisfied with the security provided by PPTP, IP Security (**IPSec**) is a more stringent standard for authorization and encryption over VPNs. If **IPSec** is used, separate clients are required, and VPN software is distributed to client machines via disk, e-mail, or a Web download. Desktop users then retrieve the client from a corporate intranet Web server. Users also must register their encryption schemes to allow coded messages to be **decoded** by corporate servers.

COMPANY NAME: Vendor Independent (999999)
SPECIAL FEATURE: Graphs
DESCRIPTORS: Computer Security; Internetworking; Network Administration; Network Software; System Monitoring; VPNs
REVISION DATE: 20020630

22/5/34 (Item 8 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00118101 DOCUMENT TYPE: Review

PRODUCT NAMES: PGP Data Security Suite 6.5.1 (764434)

TITLE: PGP encrypts the enterprise
AUTHOR: Phillips, Ken
SOURCE: PC Week, v16 n29 p81(3) Jul 19, 1999
ISSN: 0740-1604

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

Network Associates' PGP Data Security Suite 6.5.1, a full-functioned enterprise security product, gets excellent marks overall, especially for usability, capability, and performance; interoperability and manageability are rated good. Significant advantages include the ability to support most e-mail clients and mail systems; e-mail, network, and file/volume encryption with IKE and **IPSec** support; integration with X.509-enabled PKIs; a decentralized PGP infrastructure; and inclusion of a command-line client and e-mail policy manager. However, client implementation and policy updating abilities should be strengthened, and no monitoring of virtual private network (VPN) clients is provided, nor are mail client and Secure/Multipurpose Internet Mail Extensions (S/MIME) application support for Netscape and GroupWise. As shipped, PGP Data Security supports the Notes mail client and tools for sending encrypted files to non-PGP users; the latter must only enter a password to **decrypt** a file. PGP Data Security is highly scalable, and is therefore suitable for small sites with peer-to-peer configurations and large organizations that use public key infrastructure servers. An important benefit of PGP Data Security is its automated encryption for everyday tasks, which eliminates the added workload for administrators and users imposed by many other encryption and message authentication methods.

COMPANY NAME: PGP Corp (594601)
SPECIAL FEATURE: Screen Layouts Charts
DESCRIPTORS: Computer Security; Data Communications; E-Mail Utilities;

Encryption; File Transfer; Internet Security; Internet Utilities;
Network Administration; Network Software
REVISION DATE: 20040524

22/5/35 (Item 9 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00117165 DOCUMENT TYPE: Review

PRODUCT NAMES: IPSec **(836796**

TITLE: VPNs: Accent On Performance
AUTHOR: Spangler, Todd
SOURCE: Interactive Week, v6 n11 p30(1) Mar 15, 1999
ISSN: 1078-7259
HOMEPAGE: http://www.interactive-week.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

A discussion of the balance between performance and adequate network security in virtual private networks (VPNs) explains that the conventional wisdom, which dictates a sacrifice in speed in favor of encryption, may be wrong. The **Internet Protocol Security** (**IPSec**) standard under development by the Internet Engineering Task Force (IETF) is becoming more stable, and can increase the performance of commercial VPN products. One of factors that slows VPN performance is encryption, which requires resource-hungry encoding/ **decoding** of data. To address the issue, vendors are providing a new type of VPN product that is not so focused on pushing data-encrypted packets through a network as speedily as possible. Server products from Altiga Networks and Compatible Systems process thousands of concurrent users on high-bandwidth connections, while clients from 3Com and RedCreek Communications add encryption acceleration functions to client computers to ensure consistent performance over the VPN path. Component developers, including Analog Devices and Hi/fn, are developing faster, customized chips that handle **IPSec** encryption where needed. A trend toward inclusion of VPN features into networking equipment by Cisco Systems and Nortel will involve embedded support for hardware acceleration of encrypted traffic on IP routers.

COMPANY NAME: Vendor Independent (999999)
SPECIAL FEATURE: Charts
DESCRIPTORS: Communications Interfaces; Communications Standards; Computer
Security; Encryption; File Security; Firewalls; Internetworking; System
Monitoring
REVISION DATE: 20011030

22/5/36 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003 EBSCO Pub. All rts. reserv.

00612156 00NC10-405
Using Win2000's foolproof encryption -- Windows' encrypting file system lets you lock up critical data without confusing your users
Marks, Howard
Network Computing , October 30, 2000 , v11 n21 p156-158, 3 Page(s)
ISSN: 1046-4468
Company Name: Microsoft
Product Name: Microsoft Windows 2000
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Presents guidelines on using the encrypting file system (EFS) module in

the Windows 2000 operating system from Microsoft Corp. Enumerates the significant security features in Windows 2000: use of Kerberos to replace the easily-cracked LAN Manager encryption and authentication scheme, support for the industry standard IP Security (**IPSec**) virtual private network (VPN) protocols, and EFS. Indicates that all the features interact with Active Directory and the Windows 2000 public key infrastructure (PKI). Says that transparency, security, and recovery are three primary advantages of EFS. Mentions, however, that disadvantages are single-user access, heavy compute load on server, and reliance on user passwords. Details six EFS best practices, including ensuring that all files are recovered or **decrypted** before destroying recovery certificates. Includes two sidebars and a photo. (MEM)

Descriptors: Encryption; File Management; Security; Public Key Infrastructure; Virtual Private Networks; Digital Certificates

Identifiers: Microsoft Windows 2000; Microsoft

22/5/37 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus
(c)2004 Japan Science and Tech Corp(JST). All rts. reserv.

04978608 JICST ACCESSION NUMBER: 01A0890370 FILE SEGMENT: JICST-E

Making of Low Cost IPSec **Router on Linux and the Assessment for Practical Use.**

AMIKI MANABU (1); HORIO MASAHIRO (2)
(1) Sangyoidai I Igakuka; (2) Sangyoidai I Kiseichugakuvnettaiigakukyoshitsu
J UOEH Occup Environ Health, 2001, VOL.23,NO.3, PAGE.307-315, FIG.2, TBL.1, REF.20
JOURNAL NUMBER: Z0840AAP ISSN NO: 0387-821X
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02:61 621.391.037.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication

ABSTRACT: We installed Linux and FreeS/WAN on a PC/AT compatible machine to make an **IPSec** router. We measured the time of ping/ftp, only in the university, between the university and the external network. Between the university and the external network (the Internet), there were no differences. Therefore, we concluded that CPU load was not remarkable at low speed networks, because packets exchanged via the Internet are small, or compressions of VPN are more effective than encoding and **decoding** . On the other hand, in the university, the **IPSec** router performed down about 20-30% compared with normal IP communication, but this is not a serious problem for practical use. Recently, VPN machines are becoming cheaper, but they do not function sufficiently to create a fundamental VPN environment. Therefore, if one wants a fundamental VPN environment at a low cost, we believe you should select a VPN router on Linux. (author abst.)

DESCRIPTORS: LAN; computer security; data protection; internet; medical college; data compression; transmission speed; computer resource management; cryptogram; software; performance; medical data processing; cost; personal computer; response time; virtual circuit
IDENTIFIERS: virtual path; Linux; FreeS/WAN
BROADER DESCRIPTORS: computer network; communication network; information network; network; security; guarantee; protection; university; school; data processing; information processing; treatment; velocity; transmission characteristic; characteristic; management; medical information processing; digital computer; computer; hardware; time
CLASSIFICATION CODE(S): JE15030Q; ND02030R

22/5/38 (Item 1 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01500381 20010403724

Performance impact of data compression on virtual private network transactions
McGregor, JP; Lee, RB
Dept. of Electr. Eng., Princeton Univ., NJ, USA
Proceedings 25th Annual IEEE Conference on Local Computer Networks. LCN 2000, 8-10 Nov. 2000, Tampa, FL, USA2000
Document type: Conference paper Language: English
Record type: Abstract
ISBN: 0-7695-0912-6

ABSTRACT:
Virtual private networks (VPNs) allow two or more parties to communicate securely over a public network. Using cryptographic algorithms and protocols, VPNs provide security services such as confidentiality, host authentication and data integrity. The computation required to provide adequate security, however, can significantly degrade the performance. We characterize the extent to which data compression can alleviate this performance problem in a VPN implemented with the IP Security Protocol (**IPsec**). We use a system model for **IPsec** transactions to derive an inequality that specifies the conditions required for data compression to improve performance. We generate performance results for many combinations of network types, data types, packet sizes, and encryption, authentication and compression algorithms. We find that compression usually improves the performance when using 10 Mbps or slower networks, but compression only improves the performance in systems with 100 Mbps or 1 Gbps networks when using computationally intensive encryption algorithms.

DESCRIPTORS: CIPHERING-- **ENCRYPTION** ; DATA COMPRESSION; **DATA** INTEGRITY; **PACKET SWITCHING** ; COMMUNICATION NETWORKS; SAFETY; COMMUNICATION PROTOCOLS; PROTOCOLS; DATA
IDENTIFIERS: KOMMERZIELLE KOMMUNIKATION; NACHRICHTENBERECHTIGUNG; SICHERHEITSDIENST; VERTRAULICHKEIT; SYSTEMMODELL; PAKETGROESSE; AUTHENTISIERUNG; VERDICHTUNGSALGORITHMUS; 100 MEGABIT/SEKUNDE; 1 GIGABIT/SEKUNDE BEREICH; 10 MEGABIT/SEKUNDE BEREICH; Verschluesselung; Datenreduktion

22/5/39 (Item 2 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01447606 20000900753
Internet Protocol Security . **Sichere Kommunikation ueber das Internet**
Rinne, T
SSH Communications Security Corp.
LAN Line, v56, n9, pp96-99, 2000
Document type: journal article Language: German
Record type: Abstract
ISSN: 0942-4172

ABSTRACT:
Damit Unternehmen geschaeftskritische Daten sicher uebertragen koennen, wird eine standardisierte und sichere Erweiterung des Internet Protocols (IP) benoetigt. Daher hat die Internet Engineering Task force (IETF) **IPsec** verabschiedet, und zwar als Teil eines Kompendiums von Richtlinien. **IPsec** sichert die Uebertragung via TCP/IP auf der network layer (Schicht 3). Durch Umwandlung per 'Authentication Header' stellt **IPsec** sicher, dass ein akzeptiertes Datenpaket vom richtigen Absender stammt. Umwandlung per Encapsulation Security Payload verschluesselt ein Datenpaket. **IPsec** -Implementierungen muessen u. a. die Algorithmen MD5, DES und Secure Hash Algorithm anwenden. Vor dem Datenaustausch einigen die Netzknoten sich auf Verschluesselung und deren Algorithmen, Integritaet und Authentifizierung. Eine Datenstruktur namens Security Association (SA) spezifiziert, wie ein Datenpaket umgewandelt wird. Die SA wird mit einer 32-Bit-Zahl (SPI) und Kennung fuer Sender und Empfaenger gekennzeichnet. SAs werden mit dem Protokoll Internet Key Exchange (IKE) erzeugt, ausgehandelt, modifiziert und geloescht. In der ersten Phase wird einmal vorab eine SA fuer

Uebertragung gemaess Internet Security Association and Key Management Protocol (ISAKMP) erzeugt, dann in einer 2. Stufe die Sas fuer **IPsec** . Um die Gefahr zu reduzieren, dass ein Server durch ressourcenfressende Angriffe lahmgelegt wird, legt der Standard SSH **IPsec** Express fest, wie fehlerhafte Datenpakete schnell aujsgefiltert werden. **IPsec** wird von vielen IT-Anbietern unterstuetzt.

DESCRIPTORS: COMPUTER CRIME; **DATA** INTEGRITY; **PACKET SWITCHING** ;
STANDARDISATION; COMMUNICATION PROTOCOLS; CIPHERING--ENCRYPTION; INTERNET
UNIFIED COMMUNICATIONS PROTOCOL
IDENTIFIERS: **IPSEC** ; Internet; Sicherheit; Standard; **IPsec**

22/5/40 (Item 3 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01350783 I99102603300
Priority protection of wavelet transformed video over ATM
Ka-Kit Lau; Lee, MH; Ngan, KN; Rogers, G
Dept. of Electr. & Electron. Eng., Western Australia Univ., Nedlands, WA, AUS
IEEE GLOBECOM 1998 (Cat. NO. 98CH36250), 8-12 Nov. 1998, Sydney,NSW,Australia1998
Document type: Conference paper Language: English
Record type: Abstract
ISBN: 0-7803-4984-9

ABSTRACT:
We have developed an error-resilient transmission technique, called priority protection, that offers a different level of protection to each segment of an incoming data stream according to its importance. Even though a certain **group** of ATM cells are lost during transmission, the original data segment can be fully reconstructed with the protection scheme. The length of each data portion and its level of protection are user-definable in the developed simulator. We have tested the proposed scheme with a sequence of wavelet transformed images, as a wavelet transformed image consists of a number of subbands, of which each can be **classified** into a different priority level. This paper describes what the proposed scheme, priority protection, is, and how well a wavelet transformed image is protected with the scheme at a certain cell loss rate.

DESCRIPTORS: ASYNCHRONOUS TRANSFER MODE; **DATA** COMPRESSION; **PACKET SWITCHING** ; TRANSFORM **CODING** ; VIDEO CODING; WAVELET TRANSFORMS; DATA; LENGTH; SIMULATORS
IDENTIFIERS: REED SOLOMON CODE; DATENSTROM; ATM ZELLE; TEILBAND; PRIORITAETSSTUFE; ZELLENVERLUSTRATE; Asynchroner Transfermodus; Datenreduktion

22/5/45 (Item 8 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01023754 I96083389233
Video aggregation: adapting video traffic for transport over broadband networks by integrating data compression and statistical multiplexing
(Video-Aggregation: Anpassung des Video-Verkehrs fuer Breitbanduebertragungsnetze mittels Kompression und statistischem Multiplex)
Liew, SC; Chi-Yin Tse
Dept. of Inf. Eng., Chinese Univ. of Hong Kong, Shatin, Hong Kong
IEEE Journal on Selected Areas in Communications, v14, n6, pp1123-1137, 1996
Document type: journal article Language: English
Record type: Abstract
ISSN: 0733-8716

ABSTRACT:
Future broadband integrated services networks based on the asynchronous transfer mode (ATM) technology are expected to carry information from a large variety of different services and applications. This paper investigates video aggregation, a concept that integrates compression and statistical multiplexing of video information for transport over a communication network. We focus on the transmission of a **group** of video sessions as a bundle, the practical examples of which include entertainment-video broadcast and video-on-demand (VoD). In this situation, the advantage of constant bit-rate (CBR) transport (which facilitates simple network management and operation) and the advantage of variable bit-rate (VBR) video compression (which yields smoother image quality) can be achieved simultaneously. We show that it is better to integrate compression and statistical multiplexing before the bundle of video traffic enters the network than performing them as independent processes. We present experimental results which indicate the advantages of video aggregation in terms of superior image quality and efficient bandwidth usage.

DESCRIPTORS: DATA COMPRESSION; VIDEO TRANSMISSION; COMMUNICATION NETWORKS; IMAGE QUALITY; EXPERIMENTAL RESULTS; BROADBAND TRANSMISSION; BROADBAND NETWORKS; SIGNAL PROCESSING; COMMUNICATION TRAFFIC; B ISDN; CONVERSATIONAL MODE; **CODING ; FRAME TRANSMISSION ; DATA** NETWORK ADMINISTRATION; MULTIPLEXING; ASYNCHRONOUS TRANSFER MODE; VIDEO CODING; INTERACTIVE OPERATION
IDENTIFIERS: INTERACTIVE TELEVISION; INTERACTIVE VIDEO; VIDEO AGGREGATION; VIDEO TRAFFIC; STATISTICAL MULTIPLEXING; VIDEO INFORMATION; VIDEO SESSIONS TRANSPORT; ENTERTAINMENT VIDEO BROADCAST; CONSTANT BIT RATE TRANSPORT; VARIABLE BIT RATE VIDEO COMPRESSION; BANDWIDTH USAGE; BROADBAND INTEGRATED SERVICES NETWORKS; Videouebertragung; Breitbandnetz; Datenreduktion; Multiplex

22/5/46 (Item 9 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

01022639 E96096902062
ATM encryption testing
(ATM-Verschluesselungstestverfahren)
Capell, J; Deeth, D
Lockheed Martin Missiles & Space, Sunnyvale, USA
Integration Issues in Large Commercial Media Delivery Syst., Philadelphia, USA, Oct 23-24, 19951996
Document type: Conference paper Language: English
Record type: Abstract

ABSTRACT:
This paper describes why encryption was selected by Lockheed Martin Missiles & Space as the means for securing ATM (Asynchronous Transfer Mode) networks. The ATM encryption testing program is part of an ATM network trial provided by Pacific Bell under the California Research Education Network (CalREN). The problem being addressed is the threat to data security which results when changing from a packet switched network infrastructure to a circuit switched ATM network backbone. As organizations move to high-speed cell-based networks, there is a break down in the traditional security model which is designed to protect packet switched data networks from external attacks. This is due to the fact that most data security firewalls filter IP (Internet Protocol) packets, restricting inbound and outbound protocols, e.g. ftp. ATM networks, based on cell-switching over virtual circuits, does not support this method for restricting access since the protocol information is not carried by each cell. ATM switches set up multiple virtual connections, thus there is no longer a single point of entry into the internal network. The problem is further complicated by the fact that ATM networks support high-speed multimedia applications, including real-time video and video

teleconferencing which are incompatible with packet switched networks. The ability to restrict access to Lockheed Martin networks in support of both unclassified and **classified** communications is required before ATM network technology can be fully deployed. The Lockheed Martin CalREN ATM testbed provides the opportunity to test ATM encryption prototypes with actual applications to assess the viability of ATM encryption methodologies prior to installing large-scale ATM networks.

DESCRIPTORS: BROADBAND NETWORKS; BROADBAND TRANSMISSION; **INFORMATION** TRANSMISSION; **PACKET SWITCHING** ; SAFETY; **CIPHERING** --ENCRYPTION; DATA INTEGRITY; SYSTEM RELIABILITY; COMMUNICATION NETWORKS; COMMUNICATION SYSTEMS; TRANSPORT SYSTEMS; COMMUNICATION TRAFFIC; NETWORK ARCHITECTURE; EXPERIMENTAL PLANTS; TEST METHOD; CIPHERING EQUIPMENT; PROTOTYPES; SWITCHING TECHNOLOGY; SAFETY SYSTEMS; ASYNCHRONOUS TRANSFER MODE
IDENTIFIERS: asynchroner Transfer-Modus; Paketvermittlung; Sicherheit

22/5/47 (Item 10 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

00958911 E96020049233
Block permutation coding of images using cosine transform
(Block-Permutations-Codierung von Bildern mit Cosinustransformation)
Ji, Z; Tanaka, K; Kitamura, S
Kobe Univ., J
IEEE Transactions on Communications, v43, n11, pp2833-2846, 1995
Document type: journal article Language: English
Record type: Abstract
ISSN: 0090-6778

ABSTRACT:
The paper present the theory and practice of permutation coding as a new tool for very low-bit-rate image compression. Conventional source coding deals with the data information of signals, while the permutation coding achieves compression through efficiently representing the positional information (i.e., position permutation) caused by ordering the data information into order statistics. A set of four theorems is presented. The first one reveals the information-theoretic relationship between data and permutation information and the rest solves the efficient coding problem. For this, novel tools from finite **group** theory are applied to derive a compact form of representation for permutation, called permutation-cyclic-representation (PCR)-vectors, with which various regularities and constraints in the structure of positional information are displayed, whereby the coding is made very easy using a runlength and Huffman method. A block DCT-based permutation coding algorithm (the BCPC) is developed attempting to combine DCT's excellent features of energy packing and magnitude ordering that are found to be amenable to the permutation coding. This mutually benefitial characteristic significantly reduces the coding bit-rate. Simulation results are provided for real images, showing an improvement by 3-4 dB in the peak-SNR index as compared to those representing the state-of-the-art.

DESCRIPTORS: **FRAME** TRANSMISSION; **DATA** COMPRESSION; **CODING** ; DATA SIGNALLING RATE; S N RATIO; IMAGE QUALITY
IDENTIFIERS: DCT--(DISCRETE COSINUS TRANSFORMATION); Bilduebertragung; Codierverfahren; Cosinustransformation